11-06-07 AF

PTO/SB/21 (04-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	67

Application Number	09/993,135
Filing Date	11/14/2001
First Named Inventor	David Carroll Challener
Art Unit	2132
Examiner Name	Laurel L. Lashley
Attorney Docket Number	RPS9 2001 0049

ENCLOSURES (Check all that apply)

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☑ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please Identify below):

Remarks

Sent by Express Mail, Serial No. ER678749380US

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Ronald V. Davidge, Inc.		
Signature	Ronald V. Davidge		
Printed name	Ronald V. Davidge		
Date	11/03/2007	Reg. No.	33,863

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	Ronald V. Davidge		
Typed or printed name	Ronald V. Davidge	Date	11/03/2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: David Carroll Challener, et al.
Application No. 09/993,135
Filed: 11-14-2001
For: SYSTEM AND APPARATUS FOR LIMITING ACCESS TO SECURE DATA THROUGH A PORTABLE COMPUTER TO A TIME SET WITH THE PORTABLE COMPUTER CONNECTED TO A BASE COMPUTER
Group Art Unit: 2132
Examiner: Laurel L. Lashley

BRIEF ON APPEAL

Honorable Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This document is the Appellant's brief in the above described application, for which a Notice of Appeal has been accorded a receipt date of 09/05/2007.

The Director is hereby authorized to charge a fee of $510.00 for filing an appeal brief, and to charge any additional fees which may be required, and to credit any overpayment, to Deposit Account No. 50-3533. I have enclosed a duplicate copy of this sheet.

Respectfully submitted by:

Ronald V. Davidge
Registration No. 33,863
Telephone No. 954-736-0203

November 3, 2007

11/07/2007 CCHAU1 00000001 503533 09993135
01 FC:1402 510.00 DA

TABLE OF CONTENTS

Real Party of Interest

The real party of interest is Lenovo (Singapore) Pte Ltd.

Related Appeals and Interferences

There are no related appeals or interferences.

Status of Claims

Claims 1-49 are pending. No claims have been allowed.

Status of Amendments

No amendments have been filed since the Final Rejection.

Summary of the Claimed Subject Matter

Claim 1

According to the independent claim 1, a method is provided for providing access to secure data through a portable computing system (item 10 in FIG. 1, discussed on page 8, lines 6-8) during a specified time. The method comprises:

establishing a connection between said portable computing system (10) and a base computing system (item 12 in FIG. 1, discussed on page 8, lines 11-14) to provide for transfer of data between said portable computing system (10) and said base computing system (12) (in step 122 of FIG. 5A, discussed on page 16, lines 10-17);

verifying identity of said base computing system (12) within said portable computing system (10) (in step 170 of FIG. 5B, discussed on page 19, lines 19-21);

resetting a timer (as provided by the security timer subroutine 89 of FIG. 3, , discussed on page 13, line12, through page 14, line 10) within said portable computing system to run for a specified time (in step 172 of FIG. 5C, discussed on page 19, lines 21-28); and

providing access to said secure data (in step 98 of FIG. 3A, discussed on page 14, lines 10-12) only when said timer is running (as determined in step 97 of FIG. 3A, discussed on page 14, lines 7-10).

Claim 6

According to the dependent claim 6, within the method of claim 1,

said timer includes a timer register (item 88a in FIG.2, discussed on page 13, line 20, through page 14, line 4) storing a number corresponding to a time remaining,

said number corresponding to a time remaining is decremented (in step 92 of FIG. 3, described on page 13, lines 20-21) in response to a series of timing pulses generated within said portable computing system (10), and

setting said timer includes storing a number corresponding to said specified time in said timer register (step 95 in FIG. 3, discussed on page 13. lines 22-25).

Claim 7

According to the independent claim 7, a method is provided for providing for access to secure data through a portable computing system (item 10 in FIG. 1). The access to said secure data is limited to a specified time, and the method comprises:

initializing a base computing system (item 12 in FIG. 1) and said portable computing system (10) to work together as a system by an initialization process comprising;

storing data identifying said base computing system (12) within said portable computing system (10) (in step 142 of FIG. 5A); and

resetting said portable computing system (10) by a reset process following said initialization process including:

establishing a connection to transmit data between said portable computing system (10) and a base computing system (12) (in step 122 of FIG. 5A);

determining, using said data identifying said base computing system (12), that said connection has been made between said portable computing system (10) and said base computing system (12) (in step 170 of FIG. 5B);

setting a timer (as provided by the security timer subroutine 89 of FIG. 3, , discussed on page 13, line12, through page 14, line 10) within said portable computing system (10) to run until said specified time has expired (in step 172 of FIG. 5C);

determining if said timer is running (in step 97 of FIG. 3A); and

providing access to said secure data (in step 98 of FIG. 3A) only when said timer is running .

Claim 8

According to the dependent claim 8, within the method of claim 7,

said initialization process additionally includes determining whether said data identifying the base computing system has been previously stored in said portable computing system (item 10 of FIG. 1), and

if said data identifying a base computing system (item 12 of FIG. 1) is determined to have been previously stored, said data identifying a base computing system (12) remains without being overwritten during said initialization process.

Claim 10

According to the dependent claim 10, within the method of claim 8,

said timer includes a timer register (item 88a in FIG.2, discussed on page 13, line 20, through page 14, line 4) storing a number corresponding to a time remaining,

said number corresponding to a time remaining is decremented (in step 92 of FIG. 3, described on page 13, lines 20-21) in response to a series of timing pulses generated within said portable computing system, and

setting said timer includes storing a number corresponding to said specified time in said timer register (step 95 in FIG. 3, discussed on page 13. lines 22-25)..

Claim 11

According to the dependent claim 11, within the method of claim 8,

said method additionally comprises receiving an input corresponding to a time (as described on page 18, lines 5-6), and

setting said specified time according to said input.

Claim 16

According to the independent claim 16, a system is provided for providing controlled access to secure data. The system comprises:

a portable computing system (item 10 in FIG. 1, discussed on page 8, lines 6-8) providing said controlled access to secure data during a specified time, wherein said portable computing system (10) includes first processing means (item 42 in FIG. 2, discussed on page 10, lines 10-11), first storage means, and a timer (as provided by the security timer subroutine 89 of FIG. 3, , discussed on page 13, line12, through page 14, line 10);

a base computing system (12) including second processing means (also item 42 n FIG. 2, which is described as representing both the portable computing system and the base computing system) and second storage means;

a connection between said portable computing system (10) and said base computing system (12) (through the telephone network 16 of FIG. 1 or through the line 14 of FIG. 1,

discussed on page 8, lines 5-10) for transmitting data between said portable computing system (10) and said base computing system (12); and

a first program, executing within said first processing means (42), causing said portable computing system (10) to perform a process including:

determining if a public cryptographic key is stored in a first location within said first storage means (in step 130 of FIG. 5A, discussed on page 16, line 26);

in response to determining that a public cryptographic key is not stored in said first location, transmitting a request code (including the public key of the portable computing system in step 132 of FIG. 5A, discussed on page 17, lines 2-6), receiving said public cryptographic key, and storing said public cryptographic key in said first location (in step 142 of FIG. 5A, discussed on page 17, lines 16-20);

transmitting a first code (in step 152 of FIG. 5B, discussed on page 18, lines 5-6);

receiving a response to said first code (in step 156 of FIG. 5B, discussed on page 18, lines 14-15);

determining from said response to said first code if a connection has been made to said base computing system (12) (in step 170 of FIG. 5B, discussed on page 19, lines 19-21); and

a subroutine executing within said first processing means, causing said portable computing\system to perform a process including:

determining if said timer is running (in step 97 of FIG. 3A, discussed on page 14, lines 7-9); and

providing access to said secure data (in step 98 of FIG. 3A, discussed on page 14, lines 10-12) only when said timer is running;

a subroutine executing within said first processing means, causing said portable computing system to perform a process including:

determining if said timer is running (in step 97 of FIG. 3A, discussed on page 14, lines 7-9); and

providing access to said secure data (in step 98 of FIG. 3A, discussed on page 14, lines 10-12) only when said timer is running; and

a second program, executing within said second processing means, causing said base

computing system (12) to perform a process including:

receiving said request code (in step 134 of FIG. 5A, discussed on page 17, lines 7-8);

in response to receiving said request code, transmitting a public cryptographic key of said base computing system (12) to said portable computing system (10) (in step 140 of FIG. 5A, discussed on page 17, lines 12-15);

receiving said first code (in step 134 of FIG. 5A, discussed on page 17, lines 7-8); and

in response to receiving said first code, transmitting said response to said first code (in step 164 of FIG. 5B, discussed on page 19, lines 13-15).

Claim 17

According to the dependent claim 17, within the system of claim 16,

said first storage means includes a timer register (item 88a in FIG.2, discussed on page 13, line 20, through page 14, line 4) storing a number corresponding to a time remaining,

said number corresponding to a time remaining is decremented (in step 92 of FIG. 3, described on page 13, lines 20-21) in response to a series of timing pulses generated within said portable computing system, and

setting said timer includes storing a number corresponding to said specified time in said timer register step 95 in FIG. 3, discussed on page 13. lines 22-25).

Claim 29

According to the independent claim 29, a computer readable medium (such as item 57 in FIG. 2, discussed on page 11, lines 13-14) within a portable computing system (item 10 in FIG. 1, discussed on page 8, lines 6-8) is provided. Said computer readable medium has computer readable instructions for performing a method comprising:

determining if a public cryptographic key is stored in a first location within said first storage means (in step 130 of FIG. 5A, discussed on page 16, line 26);

in response to determining that a public cryptographic key is not stored in said first location, transmitting a request code (in step 132 of FIG. 5A, discussed on page 17, lines 2-6),

receiving said public cryptographic key, and storing said public cryptographic key in said first location (in step 142 of FIG. 5A, discussed on page 17, lines 16-20);

transmitting a first code (in step 152 of FIG. 5B, discussed on page 18, lines 5-6);

receiving a response to said first code (in step 156 of FIG. 5B, discussed on page 18, lines 14-15);

determining from said response to said first code if a connection has been made to a base computing system (in step 170 of FIG. 5B, discussed on page 19, lines 19-21); and

setting a timer (in step 172 of FIG. 5C, discussed on page 19, lines 21-28) to run until a specified time has expired.

Claim 30

The computer readable medium (37) of claim 29, wherein setting said timer includes storing a number corresponding to said specified time in a timer register (item 88a in FIG. 2, as described on page 13, lines 20-21).

Claim 35

According to independent claim 35, in a portable computing system (item 10 in FIG. 1, discussed on page 8, lines 6-8) having a user interface including a display (item 64 in FIG. 2, discussed on page 11, line 15) and a keyboard (item 80 in FIG 2, discussed on page 8, lines 9-10), a method for limiting access to secure data to a specified time is provided. The method comprises:

displaying a screen location (item 104 in FIG. 4, discussed on page 16, lines 3-4) for entering a number;

accepting (in step 120 of FIG. 5A, discussed on page 16, lines 9-10) an input from said keyboard (80);

displaying said input from said keyboard in said screen location (104);

calculating a number determining said specified time as a function of said input from said keyboard (80);

generating a random number (in step 144 of FIG. 5B, discussed on page 17, lines 25-27);

transmitting said random number (in step 152 of FIG. 5B, discussed on page 18, lines 5-

6) to a base computing system (item 12 in FIG. 1);

receiving (in step 156 of FIG. 5B, discussed on page 19, lines 16-17) an encrypted number from said base computing system (12),

decrypting said encrypted number with a public cryptographic key stored within said portable computing system to form a decrypted number (in step 168 of FIG. 5B, discussed on page 19, lines 19-22);

determining if said random number matches said decrypted number (in step 170 of FIG. 5B, discussed on page 19, lines 19-21); and

in response to determining that said random number matches said decrypted number, setting a timer (in step 172 of FIG. 5C, discussed on page 19. lines 21-28) within said portable computing system (10) to run for said specified time, wherein said access to secure data is provided (in step 98 of FIG. 3A, discussed on page 14, lines 10-12) only when said time is running.

Claim 37

According to independent claim 37, in a portable computing system (item 10 of FIG. 1, discussed on page 8, lines 6-8) having a user interface including a display (item 64 of FIG. 2, discussed on page 11, line 15) and a keyboard (item 80 of FIG. 80, discussed on page 11, lines 18-19), a method is provided for limiting access to secure data to a specified time. The method comprises:

displaying a first screen location (item 102 in FIG. 4, discussed on page 16, lines 7-8) for entering a password and a second screen location (item 104 of FIG. 4, discussed on page 16, lines 3-4) for entering a number;

accepting (in step 120 of FIG. 5A, discussed on page 16, lines 9-10) a first input from said keyboard (80);

generating a password from said first input;

accepting a second input from said keyboard (80);

displaying said input from said keyboard in said second screen location (104);

calculating a number determining said specified time as a function of said second input from said keyboard (80) (described on page 16, lines 4-7);

generating a random number (in step 144 of FIG. 5B, discussed on page 17, lines 25-27);

encrypting said password (in step 150 of FIG. 5B, discussed on page 18, lines 2-3) with a public cryptographic key stored in said portable computing system (10);

transmitting (in step 152 of FIG. 5B, discussed on page 18, lines 5-6) said random number to a base computing system (item 12 in FIG. 1);

receiving (in step 156 of FIG. 5B, discussed on page 18, lines 14-15) an encrypted number from said base computing system (12),

decrypting (in step 168 of FIG. 5B, discussed on page 19, lines 16-19) said encrypted number with said public cryptographic key stored within said portable computing system (10) to form a decrypted number;

determining if said random number matches said decrypted number (in step 170 of FIG. 5B, discussed on page 19, lines 19-21); and

in response to determining that said random number matches said decrypted number, setting a timer (in step 172 of FIG. 5C, discussed on page 19, lines 21-28) within said portable computing system (10) to run for said specified time, wherein said access to secure data is provided (in step 98 of FIG. 3A, discussed on page 14, lines 10-12) only when said timer is running.

Claim 44

According to independent claim 44, a portable computer (item 10 in FIG. 1, discussed on page 8, lines 6-8) is provided, including

data storage (item 88 in FIG. 2, discussed on page 12, lines 9-12) storing secure data;

communication means (item 68 in FIG. 2) for connection to a base computer (item 12 in FIG. 1, discussed on page 8, lines 11-14) for data exchange;

and processor means (item 42 in FIG. 2, discussed on page 10, lines 10-11) executing a security timer program including:

establishing a connection between said portable computing system (10) and a base computing system (12) to provide for transfer of data between said portable computing system (10) and said base computing system (12);

verifying identity of said base computing system (12) within said portable computing

system (10) (in step 170 of FIG. 5B, discussed on page 19. lines 19-21);

resetting a timer within said portable computing system (10) to run for a specified time (in step 172 of FIG. 5C, discussed on page 19, lines 21-28); and

providing access to said secure data (in step 98 of FIG. 3A, discussed on page 14, lines 10-12) only when said timer is running.

Grounds of Rejection to be Reviewed on Appeal

1. Whether Claims 1-49 are Unpatentable under 35 USC §102(e) over U.S. Patent Number 5,887.063 to Varadharajan et al.

Argument

1. Whether Claims 1-49 are Unpatentable under 35 USC §102(e) over U.S. Patent Number 5,887.063 to Varadharajan et al.

Claims 1-5, 39, and 45

The Appellant respectfully submits that U.S. Patent. No. 5,887,063 to Varadharajan et al., hereinafter *Varadharajan et al.,* fails to anticipate the requirements of claim 1 for resetting a timer within said portable computing system to run for a specified time; and for providing access to said secure data only when said timer is running.

In the Final Office Action of 04/03/2007, the Examiner disagreed with a previous assertion that *Varadharajan et al.* did not disclose resetting a timer, indicating that:

> "*Varadharajan et al.* discloses activation means responsive to the presence of the portable device that then initiates transmission of information to and from the host and portable devices. (see column 2, lines 43 - 46) *Varadharajan et al.* discloses that during communication, an activation signal produces current flow, which is logged in an audit file. It is only in the instance when the activation means receives a signal and receipt of an authenticated code from the devices that data is communicated. The audit file provides information about the transaction's origination (sender, time, etc.) (see column 5, lines 61 - 67). Since the audit file is able verify information about the transaction related to time and allowed access within a predetermined parameter (i.e. responsiveness of activation means to signaled and authenticated devices), the Examiner believes the teachings of Varadharajan et al. to be relevant to Applicant's claimed invention."

Regarding the above statement, the Appellant notes that the activation means is merely described as being responsive to the proximity of the portable device, i.e. operation of the activation means assures that the portable device has been brought into proximity with the host device. For example, the activation means may include a transducer operated by a infrared signal from the portable device or a circuit within a port receiving a signal when the portable device is plugged into the base computer. There is no indication in *Varadharajan et al* .that the

activation means only works for a specified time, or that the activation means is in any way associated with a timer. Instead, it would appear that the activation means would continue to work as needed as long as the portable device was held in proximity with the host device.

Furthermore, the Appellant notes that the use of an audit file is disclosed by *Varadharajan et al,* (in column 5, lines 60-64), only for providing security against the denial that a message was sent from the portable device. The audit file would show when each message was received. This would naturally be done using the time of day clock functions of the base computer system, with such functions being available on a typical computer system without te use of a timer that can be reset as part of the process for providing access to secure data, as required by claim 1. Additionally, it is noted that the function of supplying date and time information for the audit file occurs in the base computing system of *Varadharajan et al.*, providing no indication that a timer would be used in the portable system, as required by claim 1.

In the Final Office Action of 04/03/2007, in reference to claim 1, the Examiner further cited column 2, lines 31-42 and 59-65, FIG. 1, and the abstract of *Varadharajan et al.* However, it is noted that this material includes no reference to a timer that is set and used as required in claim 1.

For all the reasons described in detail above, the Appellant respectfully submits that the Examiner erred in determining that claim 1 was anticipated under 35 USC §102(e) by *Varadharajan et al.* Reversal of this determination is respectfully requested.

Since dependent claims 2-5, 39, and 45 add their limitations to those of claim 1, which are believed not to be anticipated as described above, the Appellant respectfully submits that the Examiner erred in determining that claims 2-5, 39, and 45 were anticipated under 35 USC §102(e) by *Varadharajan et al.* Reversal of this determination is respectfully requested.

Claim 6

The Appellant respectfully submits that *Varadharajan et al.,* fails to anticipate the requirements of dependent claim 6 for said timer to include includes a timer register storing a number corresponding to a time remaining, for said number corresponding to a time remaining to be decremented in response to a series of timing pulses generated within said portable computing system, and for setting said timer includes storing a number corresponding to said specified time

in said timer register.

As described in detail above regarding claim 1, the Appellant submits that *Varadharajan et al.* fails to describe a timer within the portable computing system.

In the Final Office Action of 04/03/2007, regarding claim 6, the Examiner cited *Varadharajan et al.*, column 3, lines 7-9, and column 4, lines 8-12.

Regarding this statement by the Examiner, the Appellant notes that, in column 3, lines 7-9, *Varadharajan et al.* says that the activation means may comprise means for detecting when said portable device is in or on or docked with said cradle or other support means. This description by *Varadharajan et al.* thus indicates a switching device indicating the presence of the portable device. For example, if the portable device were to be docked in a cradle of the base system, a switch sensing movement of the cradle under the weight of the portable device would do this.

Furthermore, the Appellant notes that, in column 4, lines 8-12, *Varadharajan et al.* says that, in embodiments including devices that can communicate both remotely and directly, the direct link is used periodically to exchange security keys, which are then used for remote communications. It is understood that "periodically" is used to indicate every so often, rather than under control of any sort of timing means, since the devices can communicate over the direct link only when they are brought together.

Therefore, the Appellant submits that these cited passages from *Varadharajan et al.* do not anticipate storing a number corresponding to a specified time within a timer.

For the reasons described above, and additionally since dependent claim 6 adds its limitations to those of claim 1, which are believed not to be anticipated as described above, the Appellant respectfully submits that the Examiner erred in determining that claim 6 was anticipated under 35 USC §102(e) by *Varadharajan et al.* Reversal of this determination is respectfully requested.

Claims 7-9, 12-15, and 40

The Appellant respectfully submits that *Varadharajan et al.*, fails to anticipate the requirements of claim 7 for setting a timer within said portable computing system to run until said specified time has expired, for determining if said timer is running, and for providing access

to said secure data only when said timer is running.

In the Final Office Action of 04/03/2007, the Examiner disagreed with a previous assertion that *Varadharajan et al.* did not disclose resetting a timer, indicating that:

> "*Varadharajan et al.* discloses activation means responsive to the presence of the portable device that then initiates transmission of information to and from the host and portable devices. (see column 2, lines 43 - 46) *Varadharajan et al.* discloses that during communication, an activation signal produces current flow, which is logged in an audit file. It is only in the instance when the activation means receives a signal and receipt of an authenticated code from the devices that data is communicated. The audit file provides information about the transaction's origination (sender, time, etc.) (see column 5, lines 61 - 67). Since the audit file is able verify information about the transaction related to time and allowed access within a predetermined parameter (i.e. responsiveness of activation means to signaled and authenticated devices), the Examiner believes the teachings of Varadharajan et al. to be relevant to Applicant's claimed invention."

Regarding the above statement, the Appellant notes that the activation means is merely described as being responsive to the proximity of the portable device, i.e. operation of the activation means assures that the portable device has been brought into proximity with the host device. For example, the activation means may include a transducer operated by a infrared signal from the portable device or a circuit within a port receiving a signal when the portable device is plugged into the base computer. There is no indication in *Varadharajan et al* .that the activation means only works for a specified time, or that the activation means is in any way associated with a timer. Instead, it would appear that the activation means would continue to work as needed as long as the portable device was held in proximity with the host device.

Furthermore, the Appellant notes that the use of an audit file is disclosed by *Varadharajan et al,* (in column 5, lines 60-64), only for providing security against the denial that a message was sent from the portable device. The audit file would show when each message was received. This would naturally be done using the time of day clock functions of the base computer system, with such functions being available on a typical computer system without te use of a timer that can be reset as part of the process for providing access to secure data, as required by claim 7. Additionally, it is noted that the function of supplying date and time

information for the audit file occurs in the base computing system of *Varadharajan et al.*, providing no indication that a timer would be used in the portable system, as required by claim 7.

In the Final Office Action of 04/03/2007, in reference to claim 7, the Examiner further cited column 2, lines 31-42 and 59-65, FIG. 1, and the abstract of *Varadharajan et al.* However, it is noted that this material includes no reference to a timer that is set and used as required in claim 7.

For all the reasons described in detail above, the Appellant respectfully submits that the Examiner erred in determining that claim 7 was anticipated under 35 USC §102(e) by *Varadharajan et al.* Reversal of this determination is respectfully requested.

Since dependent claims 8-9, 12-15, and 40 add their limitations to those of claim 7, which are believed not to be anticipated as described above, the Appellant respectfully submits that the Examiner erred in determining that claims 8-9, 12-15, and 40 were anticipated under 35 USC §102(e) by *Varadharajan et al.* Reversal of this determination is respectfully requested.

Claim 10

The Appellant respectfully submits that *Varadharajan et al.,* fails to anticipate the requirements of dependent claim 10 for said timer to include a timer register storing a number corresponding to a time remaining, for said number corresponding to a time remaining is decremented in response to a series of timing pulses generated within said portable computing system, and for setting said timer includes storing a number corresponding to said specified time in said timer register.

As described in detail above regarding claim 7, the Appellant submits that *Varadharajan et al.* fails to describe a timer within the portable computing system.

In the Final Office Action of 04/03/2007, the Examiner cited column 2, lines 43-46, and column 3, lines 7-9 regarding claim 10.

However, the Appellant notes that column 2, lines 43-48 requires activation means responsive to the presence of said portable device to cause said key update means to initiate sharing of said security key or code data via said direct communication means.

In addition, the Appellant notes that, in column 3, lines 7-9, *Varadharajan et al.* says that

the activation means may comprise means for detecting when said portable device is in or on or docked with said cradle or other support means. This description by *Varadharajan et al.* thus indicates a switching device indicating the presence of the portable device. For example, if the portable device were to be docked in a cradle of the base system, a switch sensing movement of the cradle under the weight of the portable device would do this, since the devices can communicate over the direct link only when they are brought together.

Therefore, the Appellant submits that these cited passages from *Varadharajan et al.* do not anticipate storing a number corresponding to a specified time in a register within a timer.

For the reasons described above, and additionally since dependent claim 10 adds its limitations to those of claim 7, which are believed not to be anticipated as described above, the Appellant respectfully submits that the Examiner erred in determining that claim 10 was anticipated under 35 USC §102(e) by *Varadharajan et al.* Reversal of this determination is respectfully requested.

Claim 11

The Appellant respectfully submits that *Varadharajan et al.,* fails to anticipate the requirements of dependent claim 11 for receiving an input corresponding to a time, and setting said specified time according to said input.

As described in detail above regarding claim 7, the Appellant submits that *Varadharajan et al.* fails to describe a timer within the portable computing system.

In the Final Office Action of 04/03/2007, the Examiner cited column 4, lines 9-12 of *Varadharajan et al.* regarding claim 11..

However, the Appellant notes that, in column 4, lines 9-12, *Varadharajan et al.* says that, in embodiments including devices that can communicate both remotely and directly, the direct link is used periodically to exchange security keys, which are then used for remote communications. It is understood that "periodically" is used to indicate every so often, rather than under control of any sort of timing means, since the devices can communicate over the direct link only when they are brought together.

Therefore, the Appellant submits that these cited passages from *Varadharajan et al.* do

not anticipate storing a number corresponding to a specified time according to an input.

For the reasons described above, and additionally since dependent claim 11 adds its limitations to those of claim 7, which are believed not to be anticipated as described above, the Appellant respectfully submits that the Examiner erred in determining that claim 11 was anticipated under 35 USC §102(e) by *Varadharajan et al.* Reversal of this determination is respectfully requested.

Claims 16, 21-28, and 41

The Appellant respectfully submits that *Varadharajan et al.,* fails to anticipate the requirements of claim 16 for a portable computer to include a timer, first processing means, a first program, executing within said first processing means to perform a process including setting said timer to run until said specified time has expired, and a subroutine executing within said first processing means, causing said portable computing system to perform a process including determining if said timer is running and providing access to said secure data only when said timer is running.

In the Final Office Action of 04/03/2007, the Examiner disagreed with a previous assertion that *Varadharajan et al.* did not disclose resetting a timer, indicating that:

> "*Varadharajan et al.* discloses activation means responsive to the presence of the portable device that then initiates transmission of information to and from the host and portable devices. (see column 2, lines 43 - 46) *Varadharajan et al.* discloses that during communication, an activation signal produces current flow, which is logged in an audit file. It is only in the instance when the activation means receives a signal and receipt of an authenticated code from the devices that data is communicated. The audit file provides information about the transaction's origination (sender, time, etc.) (see column 5, lines 61 - 67). Since the audit file is able verify information about the transaction related to time and allowed access within a predetermined parameter (i.e. responsiveness of activation means to signaled and authenticated devices), the Examiner believes the teachings of Varadharajan et al. to be relevant to Applicant's claimed invention."
>
> Regarding the above statement, the Appellant notes that the activation means is merely

described as being responsive to the proximity of the portable device, i.e. operation of the activation means assures that the portable device has been brought into proximity with the host device. For example, the activation means may include a transducer operated by a infrared signal from the portable device or a circuit within a port receiving a signal when the portable device is plugged into the base computer. There is no indication in *Varadharajan et al* .that the activation means only works for a specified time, or that the activation means is in any way associated with a timer. Instead, it would appear that the activation means would continue to work as needed as long as the portable device was held in proximity with the host device.

Furthermore, the Appellant notes that the use of an audit file is disclosed by *Varadharajan et al,* (in column 5, lines 60-64), only for providing security against the denial that a message was sent from the portable device. The audit file would show when each message was received. This would naturally be done using the time of day clock functions of the base computer system, with such functions being available on a typical computer system without te use of a timer that can be reset as part of the process for providing access to secure data, as required by claim 16. Additionally, it is noted that the function of supplying date and time information for the audit file occurs in the base computing system of *Varadharajan et al.*, providing no indication that a timer would be used in the portable system, as required by claim 16.

In the Final Office Action of 04/03/2007, in reference to claim 16, the Examiner further cited column 2, lines 31-42 and 59-65, col. 4, lines 1-52, FIG. 1, and the abstract of *Varadharajan et al.* In particular, column 4, lines 51-52 describe FIG. 1. However, it is noted that this material includes no reference to a timer that is set and used as required in claim 16.

For all the reasons described in detail above, the Appellant respectfully submits that the Examiner erred in determining that claim 16 was anticipated under 35 USC §102(e) by *Varadharajan et al.* Reversal of this determination is respectfully requested.

Since dependent claims 21-28 and 41 add their limitations to those of claim 16, which are believed not to be anticipated as described above, the Appellant respectfully submits that the Examiner erred in determining that claims 21-28 and 41 were anticipated under 35 USC §102(e) by *Varadharajan et al.* Reversal of this determination is respectfully requested

Claims 17-20

The Appellant respectfully submits that *Varadharajan et al.,* fails to anticipate the requirements of dependent claim 17 for said first storage means to include includes a timer register storing a number corresponding to a time remaining, for said number corresponding to a time remaining to be decremented in response to a series of timing pulses generated within said portable computing system, and for setting said timer includes storing a number corresponding to said specified time in said timer register.

As described in detail above regarding claim 16, the Appellant submits that *Varadharajan et al.* fails to describe a timer within the portable computing system.

In the Final Office Action of 04/03/2007, regarding claim 17, the Examiner cited *Varadharajan et al.,* column 2, lines 43-46, and column 3 lines 7-9. However, the Appellant notes that the activation means of column 2, lines 43-46 and of column 3, lines 7-9, is merely described as being responsive to the proximity of the portable device, i.e. operation of the activation means assures that the portable device has been brought into proximity with the host device. For example, the activation means may include a transducer operated by an infrared signal from the portable device or a circuit within a port receiving a signal when the portable device is plugged into the base computer. There is no indication in *Varadharajan et al* .that the activation means only works for a specified time, or that the activation means is in any way associated with a timer. Instead, it would appear that the activation means would continue to work as needed as long as the portable device was held in proximity with the host device.

Therefore, the Appellant submits that these cited passages from *Varadharajan et al.* do not anticipate storing a number corresponding to a specified time within a timer.

For the reasons described above, and additionally since dependent claim 17 adds its limitations to those of claim 16, which are believed not to be anticipated as described above, the Appellant respectfully submits that the Examiner erred in determining that claim 17 was anticipated under 35 USC §102(e) by *Varadharajan et al.* Reversal of this determination is respectfully requested.

Since dependent claims 18-20 add their limitations to those of claim 17, which are believed not to be anticipated as described above, the Appellant respectfully submits that the Examiner erred in determining that claims 18-20 were anticipated under 35 USC §102(e) by

Varadharajan et al. Reversal of this determination is respectfully requested

Claims 29 and 31-34

The Appellant respectfully submits that *Varadharajan et al.,* fails to anticipate the requirements of claim 29 for a computer readable medium within a portable computing system to have computer readable instructions for performing a method including determining from said first code if a connection has been made to a base computing system and setting a timer to run until a specified time has expired.

In the Final Office Action of 04/03/2007, the Examiner disagreed with a previous assertion that *Varadharajan et al.* did not disclose resetting a timer, indicating that:

> "*Varadharajan et al.* discloses activation means responsive to the presence of the portable device that then initiates transmission of information to and from the host and portable devices. (see column 2, lines 43 - 46) *Varadharajan et al.* discloses that during communication, an activation signal produces current flow, which is logged in an audit file. It is only in the instance when the activation means receives a signal and receipt of an authenticated code from the devices that data is communicated. The audit file provides information about the transaction's origination (sender, time, etc.) (see column 5, lines 61 - 67). Since the audit file is able verify information about the transaction related to time and allowed access within a predetermined parameter (i.e. responsiveness of activation means to signaled and authenticated devices), the Examiner believes the teachings of Varadharajan et al. to be relevant to Applicant's claimed invention."

Regarding the above statement, the Appellant notes that the activation means is merely described as being responsive to the proximity of the portable device, i.e. operation of the activation means assures that the portable device has been brought into proximity with the host device. For example, the activation means may include a transducer operated by a infrared signal from the portable device or a circuit within a port receiving a signal when the portable device is plugged into the base computer. There is no indication in *Varadharajan et al* .that the activation means only works for a specified time, or that the activation means is in any way associated with a timer. Instead, it would appear that the activation means would continue to work as needed as long as the portable device was held in proximity with the host device.

Furthermore, the Appellant notes that the use of an audit file is disclosed by *Varadharajan et al,* (in column 5, lines 60-64), only for providing security against the denial that a message was sent from the portable device. The audit file would show when each message was received. This would naturally be done using the time of day clock functions of the base computer system, with such functions being available on a typical computer system without te use of a timer that can be reset as part of the process for providing access to secure data, as required by claim 29. Additionally, it is noted that the function of supplying date and time information for the audit file occurs in the base computing system of *Varadharajan et al.*, providing no indication that a timer would be used in the portable system, as required by claim 29.

In the Final Office Action of 04/03/2007, in reference to claim 29, the Examiner cited *Varadharajan et al.,* column 4, lines 34-42, and column 5, lines 15-30. However, it is noted that this material includes no reference to a timer that is set and used as required in claim 29.

For all the reasons described in detail above, the Appellant respectfully submits that the Examiner erred in determining that claim 29 was anticipated under 35 USC §102(e) by *Varadharajan et al.* Reversal of this determination is respectfully requested.

Since dependent claims 31-34 add their limitations to those of claim 29, which are believed not to be anticipated as described above, the Appellant respectfully submits that the Examiner erred in determining that claims 31-34 were anticipated under 35 USC §102(e) by *Varadharajan et al.* Reversal of this determination is respectfully requested

Claim 30

The Appellant respectfully submits that *Varadharajan et al.,* fails to anticipate the requirements of dependent claim 30 for the computer readable medium of claim 29 wherein setting the timer includes storing a number corresponding to a time remaining in a timer register.

As described in detail above regarding claim 29, the Appellant submits that *Varadharajan et al.* fails to describe a timer within the portable computing system.

In the Final Office Action of 04/03/2007, regarding claim 30, the Examiner cited *Varadharajan et al.,* column 2, lines 43-46. However, the Appellant notes that the activation means of column 2, lines 43-46, is merely described as being responsive to the proximity of the

portable device, i.e. operation of the activation means assures that the portable device has been brought into proximity with the host device. For example, the activation means may include a transducer operated by an infrared signal from the portable device or a circuit within a port receiving a signal when the portable device is plugged into the base computer. There is no indication in *Varadharajan et al* .that the activation means only works for a specified time, or that the activation means is in any way associated with a timer. Instead, it would appear that the activation means would continue to work as needed as long as the portable device was held in proximity with the host device.

Therefore, the Appellant submits that these cited passages from *Varadharajan et al.* do not anticipate storing a number corresponding to a specified time within a timer.

For the reasons described above, and additionally since dependent claim 30 adds its limitations to those of claim 29 which are believed not to be anticipated as described above, the Appellant respectfully submits that the Examiner erred in determining that claim 30 was anticipated under 35 USC §102(e) by *Varadharajan et al.* Reversal of this determination is respectfully requested.

Claims 35, 36, 38, and 42

The Appellant respectfully submits that *Varadharajan et al.,* fails to anticipate the requirements of the independent claim 35 for a method for limiting access to secure dara to a specific time, with the method including calculating a number determining said specified time and of setting a timer within the portable computer system to run for said specified time, wherein access to said data is provided only when said timer is running.

The Appellant notes that, in the method of *Varadharajan et al.*, while the key exchange process is limited to a specified *condition,* that of proximity between the host system and the portable device, there is no attempt to limit the exchange of keys or data to a specified *time.*

In the Final Office Action of 04/03/2007, the Examiner disagreed with a previous assertion that *Varadharajan et al.* did not disclose resetting a timer, indicating that:

> "*Varadharajan et al.* discloses activation means responsive to the presence of the portable device that then initiates transmission of information to and from the host and portable devices. (see column 2, lines 43 - 46) *Varadharajan et al.* discloses that during

communication, an activation signal produces current flow, which is logged in an audit file. It is only in the instance when the activation means receives a signal and receipt of an authenticated code from the devices that data is communicated. The audit file provides information about the transaction's origination (sender, time, etc.) (see column 5, lines 61 - 67). Since the audit file is able verify information about the transaction related to time and allowed access within a predetermined parameter (i.e. responsiveness of activation means to signaled and authenticated devices), the Examiner believes the teachings of Varadharajan et al. to be relevant to Applicant's claimed invention."

Regarding the above statement, the Appellant notes that the activation means is merely described as being responsive to the proximity of the portable device, i.e. operation of the activation means assures that the portable device has been brought into proximity with the host device. For example, the activation means may include a transducer operated by a infrared signal from the portable device or a circuit within a port receiving a signal when the portable device is plugged into the base computer. There is no indication in *Varadharajan et al* .that the activation means only works for a specified time, or that the activation means is in any way associated with a timer. Instead, it would appear that the activation means would continue to work as needed as long as the portable device was held in proximity with the host device.

Furthermore, the Appellant notes that the use of an audit file is disclosed by *Varadharajan et al,* (in column 5, lines 60-64), only for providing security against the denial that a message was sent from the portable device. The audit file would show when each message was received. This would naturally be done using the time of day clock functions of the base computer system, with such functions being available on a typical computer system without te use of a timer that can be reset as part of the process for providing access to secure data, as required by claim 35. Additionally, it is noted that the function of supplying date and time information for the audit file occurs in the base computing system of *Varadharajan et al.*, providing no indication that a timer would be used in the portable system, as required by claim 35.

In the Final Office Action of 04/03/2007, in reference to claim 35, the Examiner cited *Varadharajan et al.,* column 4, lines 22-52 and Fig. 1. However, it is noted that this material includes no reference to a timer that is set and used as required in claim 35.

/ Since dependent claims 36, 38, and 42 add their limitations to those of claim 35, which are believed not to be anticipated as described above, the Appellant respectfully submits that the Examiner erred in determining that claims 36, 38, and 42 were anticipated under 35 USC §102(e) by *Varadharajan et al.* Reversal of this determination is respectfully requested

Claim 37 and 43

The Appellant respectfully submits that *Varadharajan et al.,* fails to anticipate the requirements of the independent claim 37 for a method for limiting access to secure data to a specified time.

The Appellant notes that, in the method of *Varadharajan et al.*, while the key exchange process is limited to a specified *condition,* that of proximity between the host system and the portable device, there is no attempt to limit the exchange of keys or data to a specified *time.*

In the Final Office Action of 04/03/2007, the Examiner disagreed with a previous assertion that *Varadharajan et al.* did not disclose resetting a timer, indicating that:

> "*Varadharajan et al.* discloses activation means responsive to the presence of the portable device that then initiates transmission of information to and from the host and portable devices. (see column 2, lines 43 - 46) *Varadharajan et al.* discloses that during communication, an activation signal produces current flow, which is logged in an audit file. It is only in the instance when the activation means receives a signal and receipt of an authenticated code from the devices that data is communicated. The audit file provides information about the transaction's origination (sender, time, etc.) (see column 5, lines 61 - 67). Since the audit file is able verify information about the transaction related to time and allowed access within a predetermined parameter (i.e. responsiveness of activation means to signaled and authenticated devices), the Examiner believes the teachings of Varadharajan et al. to be relevant to Applicant's claimed invention."

Regarding the above statement, the Appellant notes that the activation means is merely described as being responsive to the proximity of the portable device, i.e. operation of the activation means assures that the portable device has been brought into proximity with the host device. For example, the activation means may include a transducer operated by a infrared signal from the portable device or a circuit within a port receiving a signal when the portable

device is plugged into the base computer. There is no indication in *Varadharajan et al* .that the activation means only works for a specified time, or that the activation means is in any way associated with a timer. Instead, it would appear that the activation means would continue to work as needed as long as the portable device was held in proximity with the host device.

Furthermore, the Appellant notes that the use of an audit file is disclosed by *Varadharajan et al,* (in column 5, lines 60-64), only for providing security against the denial that a message was sent from the portable device. The audit file would show when each message was received. This would naturally be done using the time of day clock functions of the base computer system, with such functions being available on a typical computer system without te use of a timer that can be reset as part of the process for providing access to secure data, as required by claim 37. Additionally, it is noted that the function of supplying date and time information for the audit file occurs in the base computing system of *Varadharajan et al.*, providing no indication that a timer would be used in the portable system, as required by claim 29.

In the Final Office Action of 04/03/2007, in reference to claim 37, the Examiner cited *Varadharajan et al.,* column 4, line 12, through column 5, lines 1-15. However, it is noted that this material describes the systems and a key exchange process, wih no reference being made to a timer being set and used as required in claim 37.

Since dependent claim 43 adds its limitations to those of claim 37, which are believed not to be anticipated as described above, the Appellant respectfully submits that the Examiner erred in determining that claim 43 was anticipated under 35 USC §102(e) by *Varadharajan et al.* Reversal of this determination is respectfully requested

Claims 44 and 46-48

The Appellant respectfully submits that *Varadharajan et al.,* fails to anticipate the requirements of the independent claim 44 for a portable computer including processor means resetting a timer within said portable computing system to run for a specified time and providing access to said secure data only when said timer is running.

The Appellant notes that, in the method of *Varadharajan et al.*, while the key exchange process is limited to a specified *condition,* that of proximity between the host system and the

portable device, there is no attempt to limit the exchange of keys or data to a specified *time.*

In the Final Office Action of 04/03/2007, the Examiner disagreed with a previous assertion that *Varadharajan et al.* did not disclose resetting a timer, indicating that:

> "*Varadharajan et al.* discloses activation means responsive to the presence of the portable device that then initiates transmission of information to and from the host and portable devices. (see column 2, lines 43 - 46) *Varadharajan et al.* discloses that during communication, an activation signal produces current flow, which is logged in an audit file. It is only in the instance when the activation means receives a signal and receipt of an authenticated code from the devices that data is communicated. The audit file provides information about the transaction's origination (sender, time, etc.) (see column 5, lines 61 - 67). Since the audit file is able verify information about the transaction related to time and allowed access within a predetermined parameter (i.e. responsiveness of activation means to signaled and authenticated devices), the Examiner believes the teachings of Varadharajan et al. to be relevant to Applicant's claimed invention."

Regarding the above statement, the Appellant notes that the activation means is merely described as being responsive to the proximity of the portable device, i.e. operation of the activation means assures that the portable device has been brought into proximity with the host device. For example, the activation means may include a transducer operated by a infrared signal from the portable device or a circuit within a port receiving a signal when the portable device is plugged into the base computer. There is no indication in *Varadharajan et al* .that the activation means only works for a specified time, or that the activation means is in any way associated with a timer. Instead, it would appear that the activation means would continue to work as needed as long as the portable device was held in proximity with the host device.

Furthermore, the Appellant notes that the use of an audit file is disclosed by *Varadharajan et al,* (in column 5, lines 60-64), only for providing security against the denial that a message was sent from the portable device. The audit file would show when each message was received. This would naturally be done using the time of day clock functions of the base computer system, with such functions being available on a typical computer system without te use of a timer that can be reset as part of the process for providing access to secure data, as required by claim 44. Additionally, it is noted that the function of supplying date and time

information for the audit file occurs in the base computing system of *Varadharajan et al.*, providing no indication that a timer would be used in the portable system, as required by claim 44.

In the Final Office Action of 04/03/2007, in reference to claim 44, the Examiner cited *Varadharajan et al.,* Fig. 1, items 10 and 12, and column 2, lines 31-46 and 59-65. However, it is noted that this material describes the systems and a key exchange process, with no reference being made to a timer being set and used as required in claim 44.

Since dependent claims 46-48 add their limitations to those of claim 44, which are believed not to be anticipated as described above, the Appellant respectfully submits that the Examiner erred in determining that claims 46-48 were anticipated under 35 USC §102(e) by *Varadharajan et al.* Reversal of this determination is respectfully requested.

CLAIMS APPENDIX

1 A method for providing access to secure data through a portable computing system during a specified time, wherein said method comprises:

establishing a connection between said portable computing system and a base computing system to provide for transfer of data between said portable computing system and said base computing system;

verifying identity of said base computing system within said portable computing system;

resetting a timer within said portable computing system to run for a specified time; and

providing access to said secure data only when said timer is running.

2 The method of claim 1, wherein verifying identity of said base computing system within said portable computing system comprises:

receiving and storing a public cryptographic key from said base computing system during an initialization process,

following said initialization process, generating a random number within said portable computing system;

transmitting said random number to said base computing system;

receiving a number transmitted from said base computing system;

decrypting said number transmitted from said base computing system to form a decrypted number; and

determining that said decrypted number matches said random number.

3. The method of claim 1, additionally comprising a step of verifying whether a password is entered correctly in said portable computing system.

4. The method of claim 3, wherein said step of verifying whether a password is entered correctly includes:

transmitting an initial password to said base computing system during an initialization process,

storing said initial password within said base computing system;

following said initialization process, transmitting a present password to said base computing system;

determining in said base computing system that said initial password matches said present password;

transmitting an approval code from said base computing system to said portable computing system; and

determining that. said approval code has been received.

5. The method of claim 1, wherein said connection is established through a switched telephone network. '

6. The method of claim 1, wherein

said timer includes a timer register storing a number corresponding to a time remaining,

said number corresponding to a time remaining is decremented in response to a series of timing pulses generated within said portable computing system, and

setting said timer includes storing a number corresponding to said specified time in said timer register.

7. A method providing for access to secure data through a portable computing system, wherein said access to said secure data is limited to a specified time, and wherein said method comprises:

initializing a base computing system and said portable computing system to work together as a system by an initialization process comprising;

storing data identifying said base computing system within said portable computing system; and

resetting said portable computing system by a reset process following said initialization process including:

establishing a connection to transmit data between said portable computing system and a base computing system;

determining, using said data identifying said base computing system, that said connection has been made between said portable computing system and said base computing system;

setting a timer within said portable computing system to run until said specified time has expired;

determining if said timer is running; and

providing access to said secure data only when said timer is running.

8. The method of claim 7, wherein

said initialization process additionally includes determining whether said data identifying the base computing system has been previously stored in said portable computing system;

if said data identifying a base computing system is determined to have been previously stored, said data identifying a base computing system remains without being overwritten during said initialization process.

9. The method of claim 8, wherein said data identifying said base computing is a public cryptographic key of said base computing system, and wherein said process of determining that said connection has been made between said portable computing system and said base computing system includes:

generating and storing random number within said portable computing system;

transmitting said random number from said portable computing system to said base computing system;

encrypting said random number within said base computing system with a private cryptographic key of said base computing system to form an encrypted number;

transmitting said encrypted number from said base computing system to said portable computing system;

decrypting said encrypted number within said portable computing system with said

public cryptographic key of said base computing system to form a decrypted number; and

comparing said decrypted number with said random number stored within said portable computing system.

10. The method of claim 8, wherein

said timer includes a timer register storing a number corresponding to a time remaining,

said number corresponding to a time remaining is decremented in response to a series of timing pulses generated within said portable computing system, and

setting said timer includes storing a number corresponding to said specified time in said timer register.

11. The method of claim 8, wherein

said method additionally comprises receiving an input corresponding to a time, and

setting said specified time according to said input.

12. The method of claim 8, additionally comprising storing a cryptographic public cryptographic key of said portable computing system within said base computer system.

13. The method of claim 8, wherein

said initialization process additionally includes receiving a present password as an input, determining if a password has been previously stored, and storing said present password in response to a determination that said password has not been previously stored, .

said reset process additionally includes receiving a present password as an input and determining if said present password matches a stored password; and

said timer is set within said portable computing system only in response to a determination that said present password matches said stored password.

14. The method of claim 13, wherein

said present password is received as an input within said portable computing system,

said present password is transmitted from said portable computing system to said base computing system,

said present password is stored within said base computing system following a determination that a password is not previously stored within said base computing system;

a determination is made in said base computing system of whether said present password matches a stored password,

said reset process additionally includes transmitting an approval code from said base computing system to said portable computing system in response to a determination that said present password matches said stored password, and

said timer is set within said portable computing system in response to receiving said approval code.

15. The method of claim 14, wherein said data identifying said base computing is a public cryptographic key of said base computing system, and wherein said process of determining that said connection has been made between said portable computing system and said base

computing system includes:

generating and storing random number within said portable computing system;

concatenating said random number and said present password within said portable computing system to form a concatenated number;

encrypting said concatenated number within said portable computing system with said public cryptographic key of said base computing system to form a first encrypted number;

transmitting said first encrypted number from said portable computing system to said base computing system

decrypting said first encrypted number within said base computing system with a private cryptographic key of said base computing system to form a decrypted number;

dividing said decrypted number to form a decrypted random number and said present password;

encrypting said decrypted random number within said base computing system with a private cryptographic key of said base computing system to form a second encrypted number;

transmitting said second encrypted number from said base computing system to said portable computing system;

decrypting said second encrypted number within said portable computing system with said public cryptographic key of said base computing system to form a decrypted number; and

comparing said decrypted number with said random number stored within said portable computing system.

16. A system for providing controlled access to secure data, wherein said system comprises:

a portable computing system providing said controlled access to secure data during a specified time, wherein said portable computing system includes first processing means, first storage means, and a timer;

a base computing system including second processing means and second storage means;

a connection between said portable computing system and said base computing system for transmitting data between said portable computing system and said base computing system; and

a first program, executing within said first processing means, causing said portable computing system to perform a process including:

determining if a public cryptographic key is stored in a first location within said first storage means;

in response to determining that a public cryptographic key is not stored in said first location, transmitting a request code, receiving said public cryptographic key, and storing said public cryptographic key in said first location;

transmitting a first code;

receiving a response to said first code;

determining from said response to said first code if a connection has been made to said base computing system; and

setting said timer to run until said specified time has expired;

a subroutine executing within said first processing means, causing said portable computing system to perform a process including:

determining if said timer is running; and

providing access to said secure data only when said timer is running; and

a second program, executing within said second processing means, causing said base computing system to perform a process including:

receiving said request code;

in response to receiving said request code, transmitting a public cryptographic key of said base computing system to said portable computing system;

receiving said first code; and

in response to receiving said first code, transmitting said response to said first code.

17. The system of claim 16, wherein

said first storage means includes a timer register storing a number corresponding to a time remaining,

said number corresponding to a time remaining is decremented in response to a series of timing pulses generated within said portable computing system, and

setting said timer includes storing a number corresponding to said specified time in said timer register.

18. The system of claim 17, wherein

transmitting said first code includes generating a random number, storing said random number in a second location within said first storage, and transmitting said random number to said base computing system as said first code,

transmitting said response to said first code includes encrypting said random number with a private cryptographic key of said base computing system to form an encrypted random number, and transmitting said encrypted random number as said response to said portable computing system as said response to said first code, and

determining from said response to said first code if a connection has been made to said base computing system includes decrypting said encrypted number to form a decrypted number and comparing said decrypted number with said random number stored in said second location within said first storage.

19. The system of claim 18, wherein

said first processing means includes a first microprocessor and a first cryptographic processor,

said encrypted number is decrypted in said first cryptographic processor,

said first storage means includes first secure storage accessed only through

said first cryptographic processor, and

said first location and said timer register within said first storage means are within said secure storage.

20. The system of claim 18, wherein

said second processing means includes a second microprocessor and a second cryptographic processor,

said random number is encrypted to form said encrypted number within said second cryptographic processor,

said second storage means includes second secure storage accessed only through said second cryptographic processor, and

said private cryptographic key of said base computing system is stored within said second secure storage.

21. The system of claim 16, wherein

said portable computing system additionally includes a display,

said first program additionally causes a successful completion message to be displayed on said display in response to a determination from said response to said first code that a connection has been made to said base computing system, and

said first program additionally causes an error message to be displayed on said display in response to a determination from said response to said first code that a connection has not been made to said base computing system.

22 The system of claim 16, wherein

said portable computing system additionally includes a display and a keyboard, and

said first program causes said portable computing to perform a process additionally including displaying a menu, receiving a user input from said keyboard as said menu is displayed, and determining said specified time from said user input.

23 The system of claim 16, wherein

said portable computing system additionally includes a display and a keyboard,

said first program causes said portable computing system to perform a process additionally including displaying a menu and receiving a password from said keyboard as said menu is displayed,

transmitting said first code includes:

generating a random number;

storing said random number in a second location within said first storage;

concatenating said random number with said password to form a concatenated number

encrypting said concatenated number with a private cryptographic key of said portable computer system stored in a third location within said first storage means to form said first code; and

transmitting said random number to said base computing system as said first code, transmitting said response to said first code includes:

decrypting said first code with a private cryptographic key of said base computing system stored in a fourth location within said second storage means;

separating said password from said random number;

determining whether said password separated from said random number matches a password stored;

encrypting said random number with a private cryptographic key of said base computing system to form an encrypted random number, and

in response to determining that said password separated from said random number

matches said password stored, transmitting said encrypted random number as said response to said portable computing system as said response to said first code,

said second program causes said base computing system to perform a process additionally including:

determining if a password is stored in a fifth location within said second storage means;

in response to a determination that a password is not stored in said fifth location, storing said password separated from said random number in said fifth location;

in response to a determination that a password is stored in said fifth location, comparing said password stored in said fifth location with said password separated from said random number;

in response to determining that said password stored in said fifth location matches said password separated from said random number,

encrypting said random number and to form a transmitting an approval code to said portable computing system as said response to said first code; and

determining from said response to said first code if a connection has been made to said base computing system includes determining that said approval code has been received.

24. The system of claim 23, wherein

said second program causes said base computing system to perform a

process additionally including, in response to determining that said password stored in said fifth location does not match said password separated from said random number, transmitting an error code to said portable computing system as said response to said first code

said first program causes said portable computing to perform a process additionally including displaying a successful completion message on said display in response to receiving said approval code, and displaying an error message on said display in response to receiving said error code.

25. The system of claim 23, wherein

said first storage means includes a timer register storing a number corresponding to a time remaining,

said number corresponding to a time remaining is decremented in response to a series of timing pulses generated within said portable computing system, and

setting said timer includes storing a number corresponding to said specified time in said timer register.

26. The system of claim 23, wherein

said first processing means includes a first microprocessor and a first cryptographic processor,

said concatenated number is encrypted in said first cryptographic processor,

said first storage means includes first secure storage accessed only through said first cryptographic processor, and

said secure storage includes said first location, said third location, and said timer register within said first storage means.

27. The system of claim 23, wherein

said second processing means includes a second microprocessor and a second cryptographic processor,

said random number is encrypted to form said encrypted number within said second cryptographic processor,

said second storage means includes second secure storage accessed only through said second cryptographic processor, and

said fourth and fifth locations within said second storage means are within said second secure storage.

28. The system of claim 23, wherein

transmitting said request code includes transmitting a public cryptographic key of said portable computing system, and

receiving said request code includes storing said public cryptographic key of said portable computing system in a sixth location within said second storage means.

29. A computer readable medium within a portable computing system, wherein said computer readable medium has computer readable instructions for performing a method comprising:

determining if a public cryptographic key is stored in a first location within said first storage means;

in response to determining that a public cryptographic key is not stored in said first location, transmitting a request code, receiving said public cryptographic key, and storing said public cryptographic key in said first location;

transmitting a first code;

receiving a response to said first code;

determining from said response to said first code if a connection has been made to a base computing system; and

setting a timer to run until a specified time has expired.

30. The computer readable medium of claim 29, wherein setting said timer includes storing a number corresponding to said specified time in a timer register.

31. The computer readable medium of claim 29, wherein

transmitting said first code includes generating and storing a random number, and transmitting said random number to said base computing system as said first code, and

determining from said response to said first code if a connection has been made to a base computing system includes decrypting an encrypted number to form a decrypted number and comparing said decrypted number with said random number.

32. The computer readable medium of claim 29, wherein said method additionally comprises:

displaying a successful completion message in response to receiving an approval code; and

displaying an error message in response to receiving an error code.

33. The computer readable medium of claim 29, wherein said method additionally comprises:

displaying a menu;

receiving an input from a keyboard as said menu is displayed; and

determining said specified time from said input.

34. The computer readable medium of claim 29, wherein

said method additionally includes displaying a menu and receiving a password from a keyboard as said menu is displayed,

said step of transmitting a first code includes:

generating a random number;

storing said random number in a second location within said first storage;

concatenating said random number with said password to form a concatenated number,

encrypting said concatenated number with a private cryptographic key of said portable computer system stored in a third location within said first storage means to form said first code; and

transmitting said random number to said base computing system as said first code.

35. In a portable computing system having a user interface including a display and a keyboard, a method for limiting access to secure data to a specified time, wherein said method comprises:

displaying a screen location for entering a number;

accepting an input from said keyboard;

displaying said input from said keyboard in said screen location;

calculating a number determining said specified time as a function of said input from said keyboard;

generating a random number;

transmitting said random number to a base computing system;

receiving an encrypted number from said base computing system,

decrypting said encrypted number with a public cryptographic key stored within said portable computing system to form a decrypted number;

determining if said random number matches said decrypted number; and

in response to determining that said random number matches said decrypted number, setting a timer within said portable computing system to run for said specified time, wherein said access to secure data is provided only when said time is running.

36. The method of claim 35, additionally comprising:

displaying a successful completion message in response to determining that said random number matches said decrypted number; and

displaying an error message in response to determining that said random number does not

match said decrypted number.

37. In a portable computing system having a user interface including a display and a keyboard, a method for limiting access to secure data to a specified time, wherein said method comprises:

displaying a first screen location for entering a password and a second screen location for entering a number;

accepting a first input from said keyboard;

generating a password from said first input;

accepting a second input from said keyboard;

displaying said input from said keyboard in said second screen location;

calculating a number determining said specified time as a function of said second input from said keyboard;

generating a random number;

encrypting said password with a public cryptographic key stored in said portable computing system;

transmitting said random number to a base computing system;

receiving an encrypted number from said base computing system,

decrypting said encrypted number with said public cryptographic key stored within said portable computing system to form a decrypted number;

determining if said random number matches said decrypted number; and

in response to determining that said random number matches said decrypted number,

setting a timer within said portable computing system to run for said specified time, wherein said access to secure data is provided only when said timer is running.

38. The method of claim 35, additionally comprising:

displaying a successful completion message in response to determining that said random number matches said decrypted number; and

displaying an error message in response to determining that said random number does not match said decrypted number and in response to receiving an error code from said base system.

39 The method of claim 1, wherein said access to secure data is provided to said secure data with said portable computing system being connected to transmit and receive data from said base computing system on a periodic basis.

40. The method of claim 7, wherein said access to secure data is provided to said secure data with said portable computing system being connected to transmit and receive data from said base computing system on a periodic basis.

41. The system of claim 16, wherein said access to secure data is provided to said secure data with said portable computing system being connected to transmit and receive data from said base computing system on a periodic basis.

42. The method of claim 35, wherein, within said method, said access to secure data is

provided to said secure data with said portable computing system being connected to transmit and receive data from said base computing system on a periodic basis.

43. The method of claim 37, wherein, within said method, said access to secure data is provided to said secure data with said portable computing system being connected to transmit and receive data from said base computing system on a periodic basis.

44. A portable computer including

data storage storing secure data;

communication means for connection to a base computer for data exchange;

and processor means executing a security timer program including:

establishing a connection between said portable computing system and a base computing system to provide for transfer of data between said portable computing system and said base computing system;

verifying identity of said base computing system within said portable computing system;

resetting a timer within said portable computing system to run for a specified time; and

providing access to said secure data only when said timer is running.

45. The portable computer of claim 1, wherein said step or verifying identity of said base computing system comprises:

receiving and storing a public cryptographic key from said base computing system during an initialization process,

following said initialization process, generating a random number within said portable computing system;

transmitting said random number to said base computing system;

receiving a number transmitted from said base computing system;

decrypting said number transmitted from said base computing system to form a decrypted number; and

determining that said decrypted number matches said random number.

46. The portable computer of claim 44, additionally comprising a keyboard for data entry, wherein said method additionally comprises a step of verifying whether a password is entered correctly through said keyboard.

47. The portable computer of claim 46, wherein said step of verifying whether a password is entered correctly includes:

transmitting an initial password to said base computing system during an initialization process,

storing said initial password within said base computing system;

following said initialization process, transmitting a present password to said base computing system;

determining in said base computing system that said initial password matches said

present password;

transmitting an approval code from said base computing system to said portable computing system; and

determining that. said approval code has been received.

48. The portable computer of claim 44, wherein said connection is established through a switched telephone network.

49. The portable computer of claim 44, wherein

said timer includes a timer register storing a number corresponding to a time remaining,

said number corresponding to a time remaining is decremented in response to a series of timing pulses generated within said portable computing system, and

setting said timer includes storing a number corresponding to said specified time in said timer register.

EVIDENCE APPENDIX

This appendix includes a copy of U.S. Pat. No. 5,887,063 referenced herein.

RELATED PROCEEDINGS APPENDIX

None